

FILED

UNITED STATES DISTRICT COURT

for the
Eastern District of North Carolina

DATE 1/17/2024

PETER A. MOORE JR CLERK
USDISTRICT COURT, EDNCIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)The residence located at 3516 Rolls Avenue,
Fayetteville, North Carolina, and the silver 2000 Volvo
S80, Texas plate CV7Z847

Case No. 5:24-mj-1091-RJ

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

as further described in Attachment A.

located in the Eastern District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

Evidence of, instrumentalities used in committing, and fruits of the crimes pertaining to violations of 18 U.S.C. Section 2252A, as further described in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252A(a)(2)(A)	Receipt/Distribution of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography

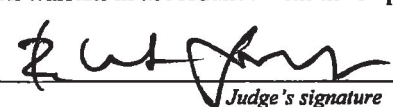
The application is based on these facts:

See attached Affidavit of Probable Cause of Special Agent Erik Bennett, AFOSI, USAF

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature
Erik A. Bennett, SA, AFOSI, USAF
Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: January 17 2024

Judge's signature
City and state: Wilmington, North CarolinaRobert B. Jones, Jr., U.S. Magistrate Judge
Printed name and title

CLW

AFFIDAVIT OF PROBABLE CAUSE

I, ERIK A. BENNETT, Special Agent, United States Air Force Office of Special Investigations (AFOSI), being duly sworn, depose and state as follows:

1. I am a Special Agent with the Department of the Air Force, Office of Special Investigations and I am currently assigned to Detachment 307, Joint Base McGuire-Dix-Lakehurst (JB MDL), NJ. I received training to be a Special Agent at the United States Air Force Special Investigations Academy (USAFSIA) and the Federal Law Enforcement Training Center (FLETC), Glynco, GA. I am conducting an investigation involving 18 U.S.C. § Section 2252A(a)(2)(A) Receipt/Distribution of Child Pornography and 18 U.S.C. § 2252A(a)(5)(B) Possession of Child Pornography (SUBJECT OFFENSES). The person I believe to be involved in the offense is identified as STEVEN LACEY (SUBJECT); Male Born: XX/XX/1986; SSN: XXX-XX-6412; 3516 Rolls Ave, Fayetteville, NC.

2. This affidavit is prepared in support of the issuance of a request for a Search Authorization that will permit me and whoever may be designated to assist, to search SUBJECT's Residence, 3516 Rolls Ave, Fayetteville, NC, a single family residence with tan and brown bricks, a shingle roof, with "3516" displayed above the two-car garage door (SUBJECT's RESIDENCE), and vehicle, a silver 2000 Volvo S80 bearing Texas license plate number CV7Z847 (SUBJECT'S VEHICLE) registered to SUBJECT. The requested search authorization seeks to seize evidence, fruits, or instrumentalities of violations of 18 U.S.C. Section 2252A(a)(2)(A) Receipt/Distribution of Child Pornography and 18 U.S.C. § 2252A(a)(5)(B) Possession of Child Pornography (SUBJECT OFFENSES).

3. The statements in this affidavit are based in part on information provided by other OSI agents and my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to

AFFIDAVIT OF PROBABLE CAUSE

me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. Section 2252A(a)(2)(A) Receipt/Distribution of Child Pornography and 18 U.S.C. § 2252A(a)(5)(B) Possession of Child Pornography (SUBJECT OFFENSES).

4. As a result of the investigation described more fully below, there is probable cause to believe that evidence, contraband, and fruits of, and other items related to, violations of the SUBJECT OFFENSES, are present or contained in the account as described in Attachment A.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. "Anime," as used herein, refers to refers to Japanese-style cartoon animation that is characterized by colorful graphics, vibrant characters, and fantastical themes, which may or may not include depictions of minors engaged in sexually explicit conduct.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in

AFFIDAVIT OF PROBABLE CAUSE

sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched.

AFFIDAVIT OF PROBABLE CAUSE

Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. “File Transfer Protocol” (“FTP”) is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP, built on client-server architecture, uses separate control and data connections between the client and the server.

h. A “hash value” is a unique alphanumeric identifier for a digital file. A mathematical algorithm, based on the file’s content, generates a hash value. A hash value is a file’s “digital fingerprint” or “digital DNA.” Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file’s hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

i. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

AFFIDAVIT OF PROBABLE CAUSE

j. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

k. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

m. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

n. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

o. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

p. A "website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hypertext Mark-up

AFFIDAVIT OF PROBABLE CAUSE

Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

q. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BIOMETRIC UNLOCKS FOR DIGITAL DEVICES

6. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time.

AFFIDAVIT OF PROBABLE CAUSE

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress Lacey's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of Lacey's face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.

Facts of the Investigation

7. LACEY is assigned to a geographically separated unit which is an operating location of the 621 Mobility Support Operations Squadron, JB MDL, NJ located at Pope Army Airfield, NC. As such, members of military law enforcement at JB MDL are charged with investigating allegations of criminal conduct wherein LACEY is the subject. On 28 Jul 2023, Ms. Gabrielle T. REED alleged to members of the Air Force, Security Forces Office of Investigations (SFOI) LACEY went through her phone and using his own phone took pictures of conversations and explicit photographs between her and Mr. Kyle PIPPIN without her knowledge or consent. In the subsequent investigation, Capt LACEY'S cell phone was seized as evidence and submitted to the United States Army Criminal Investigation Laboratory (USACIL) for examination for violations of UCMJ Article 120c: Indecent Viewing, Visual Recording, or Broadcasting pursuant to search authorization provided by Lt Col Eric B. WIETLISBACH, Commander, 621 MOBILITY SUPPORT OPERATIONS SQUADRON via AF1176 - Authority to Search and Seize. While examining the phone, Ms. Cristy Pruitt, Digital Evidence Examiner, USACIL discovered suspected child sexual abuse material (CSAM). Due to child pornography offenses being outside the investigative purview of SFOI, OSI Det 307 assumed investigative jurisdiction.

AFFIDAVIT OF PROBABLE CAUSE

a) OSI Det 307 coordinated with Ms. Cristy Pruitt, Digital Evidence Examiner, USACIL, who related she observed about six or seven images she believed to a fully nude underage female posing sexually. Ms. Pruitt described the female was pictured in a bathtub in one image and standing and facing the camera in others. Ms. Pruitt related in her capacity as a Digital Evidence Examiner she had seen these pornographic images on other devices and believed them to be of an underage female. Ms. Pruitt added she conferred with other examiners, and they believe the images to be of the actress Brooke Shields when she was 11 or 12 years old from the mass-produced film "Pretty Baby." Additionally, Ms. Pruitt disclosed she observed additional images of an unidentified female she believed to be a minor nude on her knees with her vagina exposed facing the camera. Following this conversation, OSI Det 307 obtained expanded search authorization from Lt Wietlisbach to search SUBJECT's cellular telephone for additional CSAM and provided it to USACIL.

b) On 11 Dec 23, USACIL provided a preliminary report which revealed SUBJECT's iPhone 11 Pro Max contained additional suspected CSAM which depicted photos and videos of apparent children engaged in sexual activity, posed nude or partially nude in a lewd or lascivious manner. USACIL's search revealed 17 photos of suspected CSAM and over 1,000 photos of possible CSAM. Further review was still ongoing. USACIL provided a disc containing preliminary findings to OSI Det 307 for review.

c) On 10 Jan 23, I reviewed the preliminary CSAM extracted from SUBJECT's cellular telephone, which disclosed 1,097 images labeled by USACIL examiner as suspected and possible CSAM. Examples of these files include: Photographs 1 and 2 depicted two prepubescent girls, one of which was holding open the buttocks of the other exposing her anus and vagina. Image 3 contained what appeared to be a prepubescent girl on a bed face down with her buttocks

AFFIDAVIT OF PROBABLE CAUSE

exposed and her hands spreading her buttocks exposing her anus and vagina. Image 4 depicted a fully nude prepubescent girl on a beach with her breast and vagina exposed. Image 5 depicted a prepubescent girl performing oral sex on an adult male. Image 6 depicted two prepubescent girls, nude on a beach. The two girls faced away from the camera, one of the girls sat on the others back as the girl on the bottom was on her knees. The girl on the bottom had her anus spread open exposing her anus and vagina. Additional images contained prepubescent girls posing sexually in various stages of undress. Other images depicted additional prepubescent girls performing oral sex on adult males. Some images were superimposed with logos and web addresses including 'AMOUR ANGELS;' '5 Models;' 'A Little Agency;' 'www.candydoll.tv;' 'Newstar Sunshine;' 'self-shot.cl.uk' 'doseng.org' 'sandra-earlydays.com' and 'www.RussianBare.com.' One image contained a prepubescent girl nude in a wooded area with her vagina and breasts exposed holding a cat on a leash. One image depicted a prepubescent girl in a school uniform posing in a bathroom taking a selfie of her vagina with her underwear pulled to the side. Multiple images contained prepubescent girls in staged photo shoots wearing various costumes such as maid outfits, princess outfits and lingerie.

8. Based on the information I have received through the investigation, I believe probable cause exists that a violation of 18 U.S.C. Section 2252A(a)(2)(A) Receipt/Distribution of Child Pornography and 18 U.S.C. § 2252A(a)(5)(B) Possession of Child Pornography has occurred and STEVEN LACEY was likely to have committed the offense.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ADVERTISE, TRANSPORT, DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

AFFIDAVIT OF PROBABLE CAUSE

9. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who transport, distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies, they may have, viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials or purchase childlike sex objects for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

AFFIDAVIT OF PROBABLE CAUSE

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including e-mail addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if LACEY uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in the SUSPECT RESIDENCE as set forth in Attachment A.

AFFIDAVIT OF PROBABLE CAUSE

h. Such individuals, who are known to be trading or sharing child pornography through email and other digital means, typically have a large collection in their home on a storage device such as external hard drives, cloud drives, computers with large store capacities, thumb drives and CDs. It is typical for these individuals to keep their collection of child pornography files easily accessible in order to trade with other individuals who have similar collections.

10. In view of the foregoing, your Affiant believes there is probable cause to believe that the SUBJECT OFFENSES have been violated. Accordingly, your Affiant respectfully requests that this court issue a search warrant for the listed residence more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B, which constitute evidence, contraband, fruits, and other items related to violations of the SUBJECT OFFENSES. Specifically, your Affiant request issuance of a search warrant to conduct a search of SUBJECT's RESIDENCE, described in Attachment A, and SUBJECT's VEHICLE, described in Attachment A, for electronic devices and other related evidence of the storage of CSAM material, described in Attachment B.



ERIK A. BENNETT, SA, USAF

AFOSI Detachment 307

Sworn to via telephone after submission by reliable electronic means, pursuant to Fed. R. Crim.

P. 4.1 and 41(d)(3), this 17 day of January 2024.



ROBERT B. JONES, JR.,

U.S. MAGISTRATE JUDGE, District of North Carolina

AFFIDAVIT OF PROBABLE CAUSE

ATTACHMENT A

Place to be Searched

This warrant applies to the residence 3516 Rolls Avenue, Fayetteville, NC, a one story detached single family home with a gray/black asphalt shingle roof and brick siding, with "3516" displayed above the two-car garage door.



Vehicle to be Searched

A silver in color 2000 Volvo S80 bearing Texas license plate number CV7Z847 and Vehicle Identification Number YV1TS94D8Y1118435.

AFFIDAVIT OF PROBABLE CAUSE

ATTACHMENT B

Particular Things to be Seized

I request to search and seize evidence of child sexual abuse material, including but not limited to cellular phones, electronic devices utilized to communicate or commonly used to store videos and/or electronic data, digital cameras, USBs, SD Cards, Micro SD Cards, computers, gaming consoles or anything else pertaining to child sexual abuse material.

1. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Electronic Files (or remnants of such files). Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Electronic Evidence (to include metadata). Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept

AFFIDAVIT OF PROBABLE CAUSE

in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. **Absence of Data.** The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. **Special Encryption.** Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

9. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Thus, a controlled environment with specially trained personnel may be necessary to maintain the integrity of, and to conduct a complete and accurate analysis of, data on digital devices. This process may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs

AFFIDAVIT OF PROBABLE CAUSE

that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes of data are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.